ABSTRACT

A method and system for tracing-back single packets based on storing only one record per flow, '*FlowId*', observed by a router on a given interface and in a given time window *'Time Period'*. This record can be seen as a canonical representation for all packets seen during this window. A malicious packet may be traced back to its origin by identifying the port of arrival based on that packet time of arrival *X and the FlowId*.